Configuração de filtragem de fragmentos IP de negação de serviço (DoS) em switches gerenciados 300 Series

Objetivo

O tráfego de rede é enviado por meio do uso de vários pacotes chamados datagramas. Cada método de transporte (ethernet, token ring, etc.) tem um tamanho máximo de datagrama que pode suportar. Se o datagrama for muito grande para o método de transmissão, ele será dividido em fragmentos menores. Esse processo é conhecido como fragmentação de IP. A maioria do tráfego de rede não precisa ser fragmentada. Na verdade, o tráfego que foi fragmentado pode ser usado como um ataque de negação de serviço (DoS). Um ataque de DoS inunda uma rede com tráfego falso e atrasa ou interrompe a rede. Os switches gerenciados 300 Series podem bloquear fragmentos de IP, o que diminui a vulnerabilidade das redes a um ataque de DoS. Este artigo explica como configurar as configurações de *filtragem de fragmentos IP* em Switches Gerenciados Série 300.

Note: Os filtros de fragmento IP só podem ser usados se a Prevenção de DoS estiver habilitada. Consulte o artigo *Security Suite Settings on 300 Series Managed Switches* para obter ajuda.

Dispositivos aplicáveis

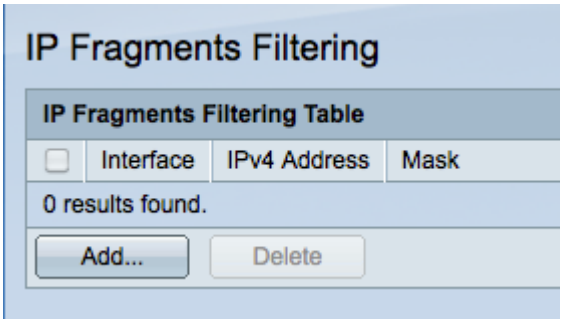
Switches gerenciados SF/SG 300 Series

Versão de software

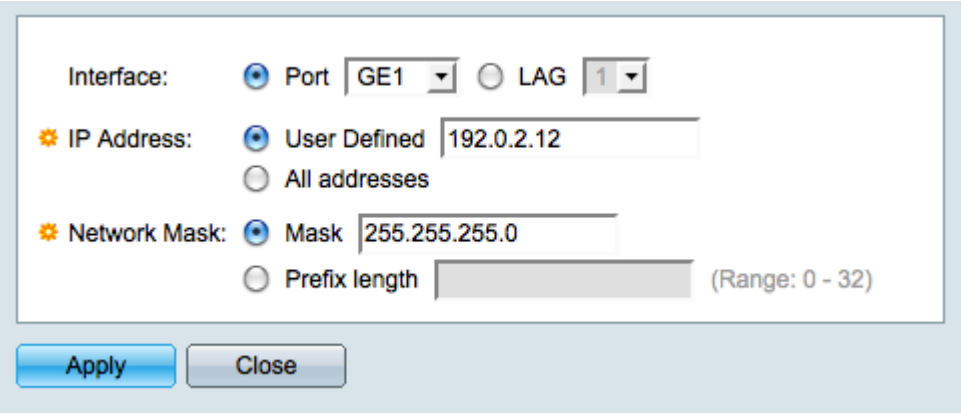
•1.3.0.62

Adicionar filtro de fragmentos de IP

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Security > Denial Of Service Prevention > IP Fragments Filtering.** A página *Filtragem de Fragmentos IP* é aberta:



Etapa 2. Clique em **Adicionar** para adicionar um novo filtro de fragmentos IP. A janela *Add IP Fragments Filtering* é exibida.



Etapa 3. Clique no botão de opção que corresponde à interface desejada no campo Interface. Esse é o local físico ao qual o filtro será atribuído.

Porta — A porta física no switch. Escolha uma porta específica na lista suspensa Porta.

LAG — Um grupo de portas que atuam como uma única porta. Escolha um LAG específico na lista suspensa LAG.

Etapa 4. Clique no botão de opção que corresponde ao endereço IPv4 desejado a ser filtrado no campo Endereço IP.

Definido pelo usuário — Insira um endereço IP a ser filtrado.

Todos os endereços — Todos os endereços IPv4 são filtrados.

Note: Se você escolheu Todos os endereços na Etapa 4, vá para a Etapa 6.

Etapa 5. Clique no botão de opção que corresponde ao método usado para definir a máscara de sub-rede do endereço IP no campo Máscara de rede.

Mask — (Máscara) Insira a máscara de rede no campo Network mask (Máscara de rede).

Comprimento do prefixo — Insira o comprimento do prefixo (inteiro no intervalo de 0 a 32) no campo Comprimento do prefixo.

Etapa 6. Clique em **Apply** para salvar suas alterações e clique em **Close** para fechar a janela *Add IP Fragments Filtering (Adicionar filtragem de fragmentos de IP)*.